

FILED

RICHARD W. NAGEL
CLERK OF COURT

UNITED STATES DISTRICT COURT

for the
Southern District of Ohio

12/17/20

U.S. DISTRICT COURT
SOUTHERN DIST. OHIO
WEST. DIV. DAYTONIn the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)INFORMATION ASSOCIATED WITH 11 GMAIL
ACCOUNTS, THAT ARE STORED AT PREMISES
CONTROLLED BY GOOGLE

Case No.

2:20-mj-572

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

SEE ATTACHMENT A

located in the Southern District of Ohio, there is now concealed (identify the person or describe the property to be seized):

SEE ATTACHMENT B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. § 1341	Mail Fraud
18 U.S.C. § 1343	Wire Fraud
18 U.S.C. § 1028A	Aggravated Identity Theft

The application is based on these facts:

SEE ATTACHED AFFIDAVIT

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days:
18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

is requested under

Applicant's signature

SA Kim Martinez
Printed name and titleAttested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by
(specify reliable electronic means).Date: 12/15/2020 12-17-20 cmv

Judge's signature

City and state: Columbus, OhioChelsey M. Vascara, U.S. Magistrate Judge
Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH
BKAWESOME6969@GMAIL.COM,
BKBATMAN69@GMAIL.COM,
BKMONALISA69@GMAIL.COM,
BKROBINHOOD69@GMAIL.COM,
BKSOLID6969@GMAIL.COM,
BUILDERSROBERT@GMAIL.COM,
BW0025891@GMAIL.COM,
KARENDEY208@GMAIL.COM,
MCRUZ19701970@GMAIL.COM,
MONACENTER65@GMAIL.COM,
TAISHABRUNSON054@GMAIL.COM
THAT IS STORED AT PREMISES
CONTROLLED BY GOOGLE.

3:20-mj-572

Case No. _____

Filed Under Seal

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Kim Martinez, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with [a] certain account[s] that is stored at premises controlled by Google LLC an email provider headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google LLC to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. Your Affiant is a Special Agent with the United States Secret Service, and have been since May 11, 2016. I have completed the Criminal Investigator Training Program and the Customs and Border Protection Officer Training Program at the Federal Law Enforcement Training Center in Glynco, GA and the Special Agent Training Course at the James J. Rowley Training Center in Laurel, MD. I have also completed additional training courses to include: Basic Investigation of Computer and Electronic Crimes Program at the James J. Rowley Training Center, Business Email Compromise and Ransomware Investigations through the National Computer Forensic Institute, Network Layer 1 & 2 Troubleshooting through Federal Virtual Training Environment, Ports, Protocols, and the OSI Model for Network+, Policies and Best Practices for Network+, and Operational Use of Social Media in the Performance and Learning Management System's online training with the United States Secret Service; IT Concepts, Programming in C, and Symbolic Computations in Mathematics (covering the programming systems Maple and Mathematical) at the University of South Florida; and Basic Computer Skills at Saint Leo University. I am presently assigned the responsibility of investigating violations of federal law, including those violations pertaining to computer fraud, wire fraud, and mail fraud.

3. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 1341 (mail fraud); 18 U.S.C. §; 1343 (wire fraud); and 18 U.S.C. § 1028A (aggravated identity theft) have been committed by Kenneth Wilson or Brandi Sweet. There is also probable cause to search the information described in Attachment A for evidence of these crimes further described in Attachment B.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

6. On August 21, 2020 in the Southern District of Ohio, law enforcement officers with the Brookville Police Department conducted a traffic stop on a blue 1992 GMC pickup truck bearing Ohio registration HUV3297 for failure to signal.

7. Contact was made with the driver of the vehicle, later identified as Kenneth Wilson, and the passenger of the vehicle, later identified as Brandi Sweet.

8. Officers observed that the bed of the truck was full of miscellaneous items. Officers asked Wilson about the items in the bed of the truck, and Wilson told officers that he had cleaned out his storage locker.

9. Sweet told officers that the items were from their (Sweet and Wilson’s) storage locker and that they intended to sell them at a flea market.

10. Wilson provided officers with an Ohio State Identification card with the name David Christopher Campbell on it. Wilson told officers that his Ohio driver’s license had been suspended. Officers returned to their patrol vehicle to confirm the identities of the individuals in the truck.

11. Officers checked the vehicle's registration and learned that Ohio registration HUV3297 was associated with a red 2006 GMC truck and was registered to an Edwin Humphrey.

12. Officers attempted to return to the blue truck when Wilson put the truck into drive and fled the scene.

13. Officers pursued the truck for a time, but ended the pursuit unsuccessfully due to the speed of the pursuit and the traffic conditions at the time.

14. Later the same evening, officers with the Huber Heights Police Department spotted the blue truck and re-initiated pursuit. During that pursuit the blue truck crashed. Officers from the Brookville Police Department responded to the crash site.

15. The Huber Heights officers advised the Brookville Police Department that the blue truck had crashed, and that both the driver and the passenger had fled the crash on foot. Huber Heights officers had taken the passenger, Sweet, into custody, but the driver had successfully escaped. Located near the truck was a purse, in that purse was a cellular telephone.

16. Brookville officers interviewed Sweet. Sweet initially identified the driver of the blue truck as David Campbell. Later in the interview, however, Sweet admitted that the driver of the vehicle was Wilson. In Sweet's possession was a cellular telephone. Also in Sweet's possession was an Ohio driver's license for McKayla Lynn Jordan.

17. Officers learned that the blue truck had been stolen from the Prebco Towing impound lot after having been subject to a tow request from the Preble County Sheriff's

Department when the occupant at the truck at that time (neither Wilson nor Sweet) had been arrested for OVI.

18. Brookville officers obtained a warrant and searched the blue truck. Among numerous other items located in the bed of the truck, officers found a blue wheel tote containing numerous files. Also in the bed of the truck, officers located a notebook. In the cab of the truck, officers located an additional cell phone near the driver's seat. Visible on the screen of the cell phone was a message from a "Cody" at the Deerfield Inn at 2871 U.S. 35 West Alexandria, Ohio.

19. Officers contacted the Deerfield Inn at 2871 U.S. 35 West Alexandria. They were informed that the room was rented to a McKayla, but that she was known as "Brandi." Also staying in the room was a Kenneth Wilson.

20. Officers learned that files in the blue wheel tote were employee files of certain former employees of Schaffner Manufacturing. The files contained personal identifying information such as the birth dates, names, and social security numbers of the former employees.

21. The following employee files were recovered:

- Joni Ansel
- Sherman Bailey
- Kenneth Banks
- Richard Brown
- Taisha Brunson
- Victor Carrero-Cuevas
- Marquis Cobbs

- Rachel Cruz
- Alexander Cvjetcanin
- Lonnie Davis
- Marcus Deloney
- Edward Dieterich
- Regis Donahue
- Rodlyn Dunson
- William Fincher
- Cornelius Green
- Synthia Hardin
- Debra Lynn Harris

22. Officers made contact with Osborn Manufacturing, the successor to Schaffner Manufacturing, and learned that the files had been taken in a break-in at a storage unit in Richmond, Indiana on July 29, 2020.

23. The notebook contained several pages of writing. Among those pages is the following information:

- A page which states “Brandi [heart drawing]’s Kenny.”
- A list of email addresses and associated names, including:
bkaweseome6969@gmail.com (Karen Dey); bkmonalisa69@gmail.com (Mona Lisa); bkrobinhood69@gmail.com (Robin Hood); bkbatman69@gmail.com (Bruce Wayne); bksolid6969@gmail.com (Bonnie Clyde);

karendey208@gmail.com (Karen Dey); bw0025891@gmail.com (Bruce Wayne);
monacenter65@gmail.com (Mona Center).

- Underneath bw0025891@gmail.com is the parenthetical annotation “Edward Dieterich.” Underneath monacenter65@gmail.com is the parenthetical annotation “Rachel Cruz.” Edward Dieterich and Rachel Cruz were the names of two employees whose files were stolen.
- There is an additional email address, mrcruz19701970@gmail.com. Included near that email address is the annotation “[XXX] [XX] 2563.” This annotation is consistent with the social security number contained in Rachel Cruz’s employee file.
- The annotation “2871 US 35 West Alex OH 45381,” which is the address of the Deerfield Inn.

24. A subpoena was sent to Google for all email addresses found in the notebook, and select additional email addresses. The returns for that subpoena revealed, *inter alia*:

<u>Email Address</u>	<u>Account Name</u>	<u>Create Date</u>	<u>Terms of Service IP Address</u>
<u>hkawesome6969@gmail.com</u>	[none]	8/2/2020	[none]
<u>bkbatman69@gmail.com</u>	Bruce Wayne	8/2/2020	2607:fb90:62e4:d936:ddaa:52e3:131a:4b35
<u>bkmonalisa69@gmail.com</u>	Mona Lisa	8/2/2020	2607:fb90:62e4:d936:ddaa:52e3:131a:4b35
<u>bkrbinhood69@gmail.com</u>	Robin Hood	8/2/2020	2607:fb90:62e4:d936:ddaa:52e3:131a:4b35
<u>bksolid6969@gmail.com</u>	Bonnie Clyde	8/2/2020	2607:fb90:62e4:d936:ddaa:52e3:131a:4b35
<u>buildersrobert@gmail.com</u>	Robert Builders	8/2/2020	2607:fb90:62e4:d936:ddaa:52e3:131a:4b35
<u>bw0025891@gmail.com</u>	Bruce Wayne	8/2/2020	2607:fb90:62e4:d936:ddaa:52e3:131a:4b35
<u>karendey208@gmail.com</u>	Karen Dey	8/2/2020	2607:fb90:62e4:d936:ddaa:52e3:131a:4b35
<u>mrcruz19701970@gmail.com</u>	my shiznit n[****]	8/4/2020	2607:fb90:2b03:8ce4:0:15:87c7:8a01
<u>monacenter65@gmail.com</u>	Mona Center	8/2/2020	2607:fb90:62e4:d936:ddaa:52e3:131a:4b35
<u>taishabrunson054@gmail.com</u>	Taisha Brunson	8/7/2020	2607:fb90:6240:c5dc:0:d:c9b8:4601

25. Officers also conducted certain additional investigation and learned that Pandemic Unemployment Assistance (“PUA”) claims had been made in the names of Taisha Brunson and Rachel Cruz.

26. The claim for Rachel Cruz was filed on August 4, 2020. It provided a mailing address of 2871 U.S. 35, West Alexandria, OH. The associated email address was monacenter650@gmail.com.¹

27. The claim for Taisha Brunson was filed on August 7, 2020. It provided a mailing address of 2871 U.S. 35, West Alexandria, OH. The associated email address was taishabrunson054@gmail.com.

28. Prior to sending a subpoena, a preservation request was sent to Google LLC for all Target Email Addresses. In general, an email that is sent to a Gmail subscriber is stored in the subscriber’s “mail box” on Google LLCs’ servers until the subscriber deletes the email. If the subscriber does not delete the message, the message can remain on Google LLC’s servers indefinitely. Even if the subscriber deletes the email, it may continue to be available on Google LLC’s servers for a certain period of time. The subpoena returns revealed that all Target Email Addresses except for bkawesome6969@gmail.com were active at the time of the preservation request. The subpoena returns showed that the bkawesome6969@gmail.com account was deleted a few minutes after creation.

¹ A subpoena to Google for that email address returned no results. Results were obtained for the email address monacenter65@gmail.com and are summarized in the table above.

BACKGROUND CONCERNING EMAIL

29. In my training and experience, I have learned that Google LLC provides a variety of on-line services, including electronic mail ("email") access, to the public. Google LLC allows subscribers to obtain email accounts at the domain name gmail.com, like the email account[s] listed in Attachment A. Subscribers obtain an account by registering with Google LLC. During the registration process, Google LLC asks subscribers to provide basic personal information. Therefore, the computers of Google LLC are likely to contain stored electronic communications (including retrieved and unretrieved email for Google LLC subscribers) and information concerning subscribers and their use of Google LLC services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

30. A Gmail subscriber can also store with the provider files in addition to emails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to emails), and other files, on servers maintained and/or owned by Google LLC. In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, email in the account, and attachments to emails, including pictures and files.

31. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information

can be used to identify the account's user or users. Based on my training and my experience, I know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities. In this case, subpoena returns have already revealed that many of the names associated with the Target Email Addresses on the Google LLC servers are consistent with the associated names and email accounts written down in the notebook found in the 1992 GMC blue pickup truck.

32. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (*i.e.*, session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account. In this case, the subpoena returns indicate that Google LLC does record and store this information. .

33. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as

a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

34. As explained herein, information stored in connection with an email account may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculcate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (*e.g.*, location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in

the email account may indicate the owner's motive and intent to commit a crime (*e.g.*, communications relating to the crime), or consciousness of guilt (*e.g.*, deleting communications in an effort to conceal them from law enforcement). In this case, the application for PUA benefits requires the applicant to provide an email address with their application, and may use that email address to communicate with the applicant. The contents of the Target Email Addresses may reveal which accounts were used to set up PUA applications or any communications the users of the Target Email Addresses had concerning any PUA applications or benefits. Additionally, the IP data associated with those accounts may connect the users of the phone to a certain location, such as the Deerfield Inn.

CONCLUSION

35. Based on the forgoing, I request that the Court issue the proposed search warrant.

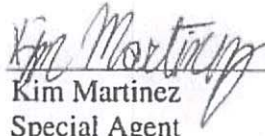
36. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Google LLC. Because the warrant will be served on Google LLC, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

REQUEST FOR SEALING

37. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee/continue flight from

prosecution, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.


Respectfully submitted,



Kim Martinez

Special Agent
United States Secret Service

Subscribed and sworn to before me on 12-17, 2020



Honorable Chelsey Vascura
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with BKAWESOME6969@GMAIL.COM, BKBATMAN69@GMAIL.COM, BKMONALISA69@GMAIL.COM, BKROBINHOOD69@GMAIL.COM, BKSOLID6969@GMAIL.COM, BUILDERSROBERT@GMAIL.COM, BW0025891@GMAIL.COM, KARENDEY208@GMAIL.COM, MCRUZ19701970@GMAIL.COM, MONACENTER65@GMAIL.COM, TAISHABRUNSON054@GMAIL.COM that is stored at premises owned, maintained, controlled, or operated by Google, a company headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Google LLC (the “Provider”)

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to requests made under 18 U.S.C. § 2703(f) on October 23, 2020, October 30, 2020, and November 6, 2020 (Google Reference #4134573, 4161091, & 4607473) the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. The contents of all emails associated with the account from July 29, 2020 to the present, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. The types of service utilized;

d. All records or other information stored by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files; and

e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken. The Provider is hereby ordered to disclose the above information to the government within **14 days** of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes evidence or instrumentalities of violations of **18 U.S.C. § 1341 (mail fraud); 18 U.S.C. §; 1343 (wire fraud); and 18 U.S.C. § 1028A (aggravated identity theft)**, those violations involving Kenneth Wilson or Brandi Sweet and occurring on or after July 29, 2020, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- a. any information demonstrating possession, use, or access to the Schaffner employee files for the following individuals:

- Joni Ansel
- Sherman Bailey
- Kenneth Banks
- Richard Brown
- Taisha Brunson
- Victor Carrero-Cuevas
- Marquis Cobbs
- Rachel Cruz
- Alexander Cvjetcanin
- Lonnie Davis
- Marcus Deloney
- Edward Dieterich
- Regis Donahue
- Rodlyn Dunson
- William Fincher
- Cornelius Green

- Synthia Hardin
 - Debra Lynn Harris
- b. any information related to the use of the identifying information contained in the Schaffner employee files to apply for public benefits, including unemployment assistance;
 - c. any information related to the user of the Target Email Addresses' receipt of public benefits, including unemployment assistance;
 - d. any information demonstrating the user of the Target Email Addresses' residence in, use of, access to, or receipt of mail at the Deerfield Inn at 2871 U.S. 35, West Alexandria, OH.
 - e. any information recording Kenneth Wilson or Brandi Sweet's schedule or travel from July 29, 2020 to the present;
 - f. any information showing communication between Kenneth Wilson and Brandi Sweet;
 - g. any location data showing the location of the Target Email Addresses' user from July 29, 2020 to the present;
 - h. all bank records, checks, credit card bills, account information, and other financial records.
 - i. Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;

- j. Evidence indicating the email account owner's state of mind as it relates to the crime under investigation;
- k. The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).
- l. The identity of the person(s) who communicated with the user ID about matters relating to the application or receipt of public benefits, including unemployment assistance, including records that help reveal their whereabouts.
- m. Records evidencing the use of Internet Protocol addresses to access Gmail accounts; send specific messages; or apply for public benefits, including unemployment assistance.

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC
RECORDS PURSUANT TO FEDERAL RULES OF
EVIDENCE 902(11) AND 902(13)**

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by Google LLC, and my title is _____.

I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Google LLC. The attached records consist of _____ the contents of the Target Email Addresses. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of Google LLC, and they were made by Google LLC as a regular practice; and

b. such records were generated by Google LLC's electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of Google LLC in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by Google LLC, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

Date

Signature